CYBERSECURITY THREAT INTELLIGENCE

Weekly Assessment Report |
Period Ending August 21, 2025

CODEC NETWORKS CONFIDENTIAL

Generate
8/21/2025, 3:21:
P
Report ID: C
JX0XTN

THREAT LEVEL: ELEVATED

Threat Landscape

3 critical incidents contained • 1 APT indicator detected • 14 CVEs require immediate attention

Security Posture

Alert volume ↓12% • MTTA 21m • MTTR 4h12m • EDR coverage 85%

Compliance Status

PCI DSS 88% compliant • NIST 800-53 84% compliant • 7 controls failing

KEY METRICS

TOTAL ALERTS

4,820

↓12% vs last week

CRITICAL ALERTS

18

↓8% vs last week

MTTA

21m

Mean Time to Acknowledge

MTTR

4h 12m

Mean Time to Resolution

FALSE POSITIVES

6%

Alert accuracy

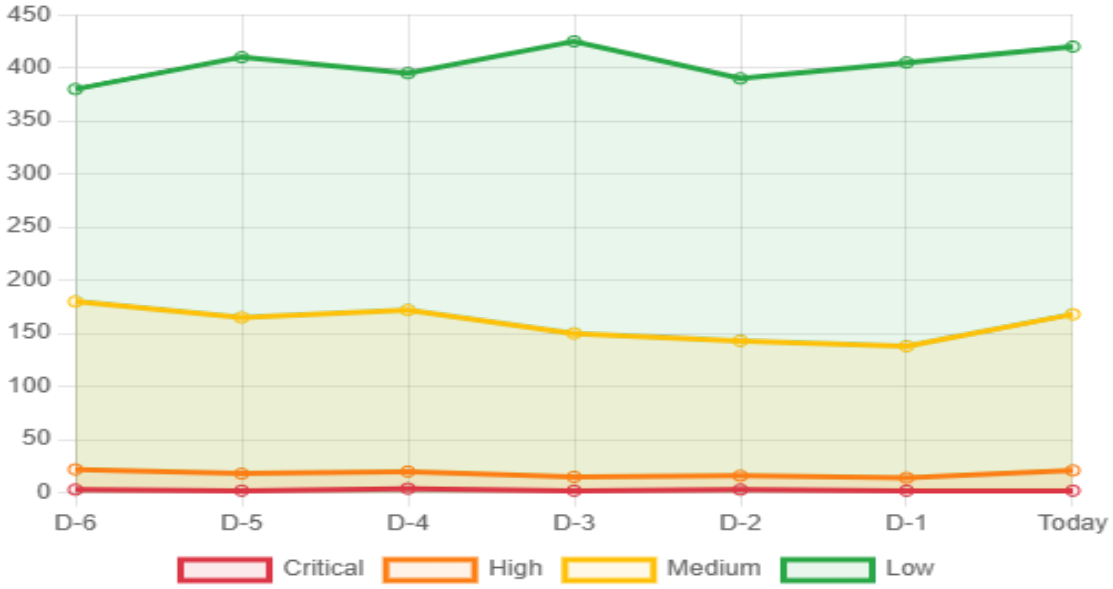
EDR COVERAGE

85%

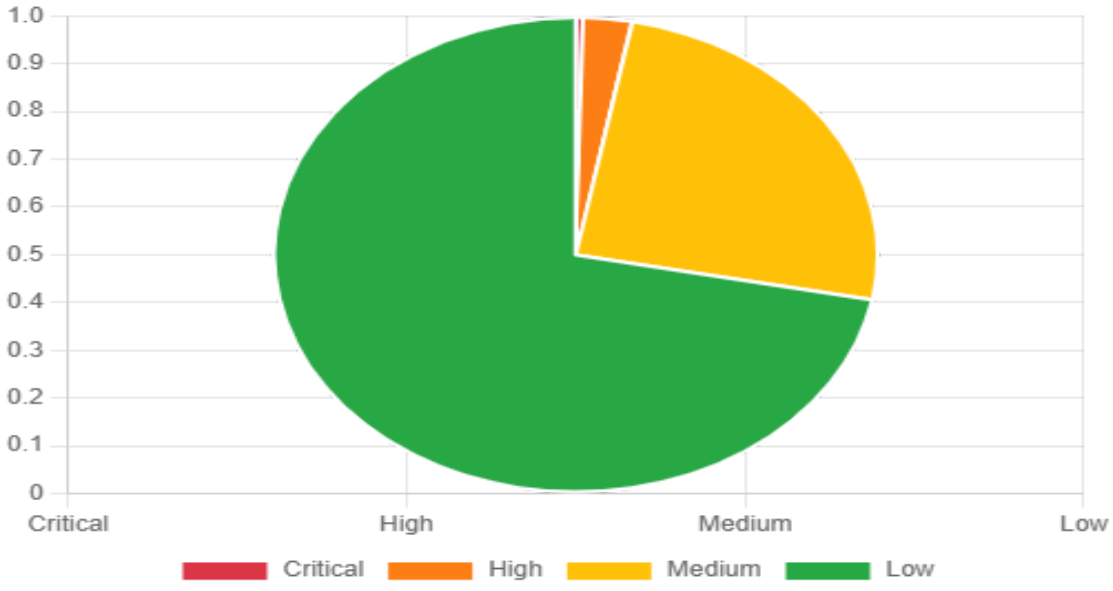
Endpoint protection

SECURITY TRENDS & ANALYSIS

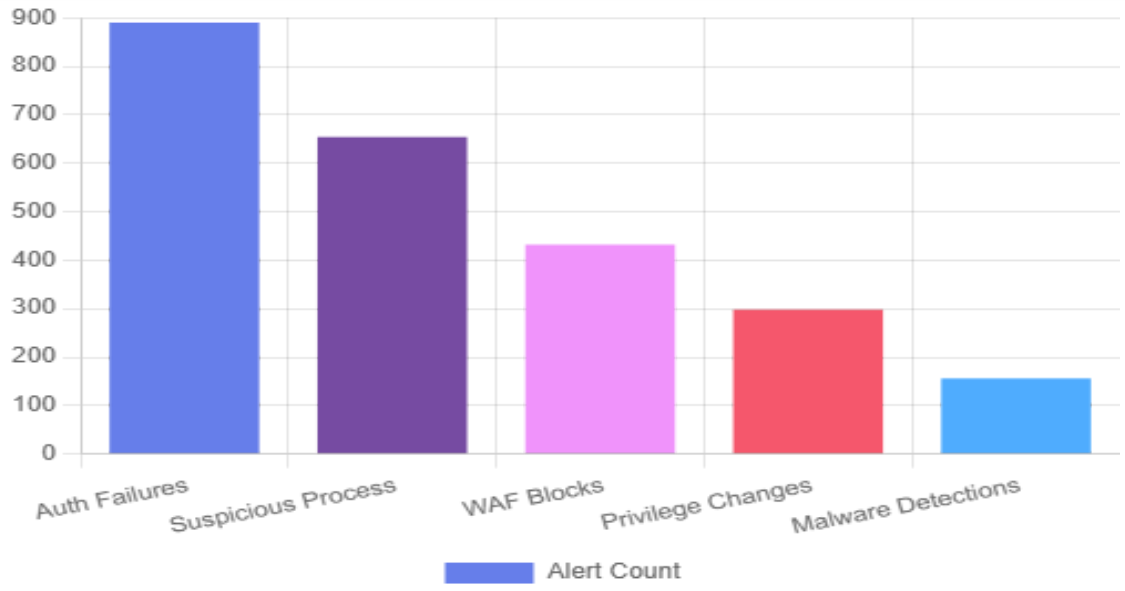
Alerts per Day (Stacked by Severity)



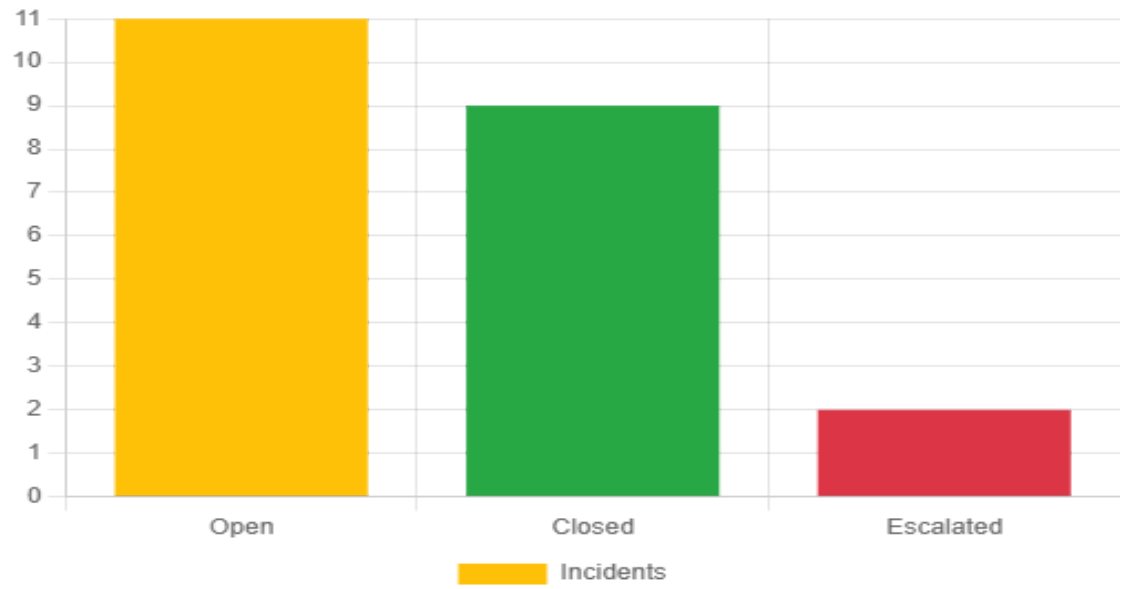
Alert Severity Distribution



Top Alert Categories



Incidents by Status



TOP NOISY ASSETS

Asset	Role	Total Alerts	Critical	High
web-01	Frontend	612	4	21
api-02	API	558	3	18
db-01	Database	410	2	15
vpn-gw	VPN	392	1	22
idm-01	Identity	375	3	17

INCIDENTS & INVESTIGATIONS

Lateral Movement Attempt Blocked

Timeline: D-2 14:22–16:05 IST
Root cause: Compromised contractor account; password reuse detected.
Impact: 3 endpoints targeted; no data exfiltration.
Status: Contained; creds rotated; device reimaged.
Evidence: Wazuh Search ID 78321; Case ID INC-2025-0819-01.

Suspicious PowerShell on Finance Host

Timeline: D-4 10:11–10:19 IST
Root cause: Malicious macro executed by user.
Impact: No persistence; blocked by EDR.
Status: Closed; user retrained.
Evidence: Wazuh Search ID 78104; EDR Alert 4472.

Excessive Authentication Failures (VPN)

Timeline: D-1 06:30–08:00 IST
Root cause: Credential stuffing from 3 ASNs.
Impact: No successful logins.
Status: Mitigated; WAF/Geo rules updated; rate-limit enabled.
Evidence: NetSec Rule Update CHG-5521.

COMPLIANCE POSTURE

PCI DSS

88%

Failing controls:

- 8.1.4 MFA for privileged access incomplete on 12 users
- 10.2.5 Logging gaps on 3 Linux servers
- 11.2.1 Quarterly ASV scan exceptions pending

NIST 800-53

84%

Failing families:

- AC-2 (Account Management) – weak deprovisioning cadence
- AU-6 (Audit Review) – incomplete centralization for legacy hosts
- SI-2 (Flaw Remediation) – overdue patches on db-01/api-02

RECOMMENDATIONS

Quick Wins (≤2 weeks)

Enforce MFA for all privileged users

CRITICAL

OWNER	ETA	RISK REDUCTION
IAM Lead	7 days	High

EFFORT

Medium

Patch OpenSSL on web/api tier

CRITICAL

OWNER	ETA	RISK REDUCTION
App Ops	3 days	High

EFFORT

Low

Close SSH from 0.0.0.0/0 in 3 security groups

CRITICAL

OWNER	ETA	RISK REDUCTION
NetSec	2 days	High

EFFORT

Low

Push EDR agent to 15 uncovered endpoints via MDM

MEDIUM

OWNER	ETA	RISK REDUCTION

EUC | 5 days | Medium

EFFORT
Medium

Enable lockout/rate-limit on VPN; block hostile ASNs

MEDIUM

OWNER	ETA	RISK REDUCTION
NetSec	2 days	Medium

EFFORT
Low

Strategic (>2 weeks)

Implement least-privilege cleanup and automated deprovisioning

CRITICAL

OWNER	ETA	RISK REDUCTION
IAM	4 weeks	High

EFFORT
High

Centralize Linux audit policy and forwarders to raise PCI 10.x pass rate

MEDIUM

OWNER	ETA	RISK REDUCTION
Platform	3 weeks	Medium

EFFORT
Medium

Quarterly internet-exposed vuln review with CAB-approved emergency windows

CRITICAL

OWNER	ETA	RISK REDUCTION
SecOps	6 weeks	High

EFFORT

Medium

Expand EDR health SLOs and auto-remediation

MEDIUM

OWNER	ETA	RISK REDUCTION
SecEng	5 weeks	Medium

EFFORT

High

d forwarders

Owner: Platform | ETA: 3 weeks | Risk Reduction: Medium

Quarterly internet-exposed vuln review

Owner: SecOps | ETA: 6 weeks | Risk Reduction: High

Expand EDR health SLOs and auto-remediation

Owner: SecEng | ETA: 5 weeks | Risk Reduction: Medium

APPENDIX

Evidence references:

- Wazuh Search IDs: 78104, 78321, 78490
- Ticket IDs: INC-2025-0819-01, CHG-5521
- Report generated:

Implementation notes:

- Rendering: Charts generated using Chart.js with consistent metrics
- Download: HTML→PDF conversion with immediate download trigger
- Flags: Sample data watermark until connected to live data sources